


Background

When On-Prem AD and AzureAD are connected one new on-prem account is created, and one new AzureAD account is created.

On-prem account is called `MSOL_` -and then some random string. This account has DCSync privileges, and should therefore be considered a tier 0 resource.

MSOL-account can perform syncornization with AzureAD. The synchronization job is performed on a server. Which server that is is disclosed in the description attribute of the MSOL-user. It says something like:

```
Account created by Microsoft Azure Active Directory Connect with installation identifier <RANDOM STRING> running on computer <NAME C
```

A screenshot of a text field with a scrollbar. The text is truncated on the right side, and the scrollbar is visible on the right edge of the field.

By compromising the server or the account it is possible to perform a DCSync attack.

Pre-requisites

Risks

How to check for

How to exploit

Recommendation

Related Vulnerabilities

This finding should not be reported as the name of this issue, instead it should be reported as the vulnerabilities written below. The below written vulnerabilities map to the vulnerability-descriptions in that repo.

For example, if kerberoast, report as the following vulnerabilities if they are applicable:

- Weak password [ID of issue]
- Overpriviliged kerberoastable user [ID of issue]

References
